VZCZCXRO8134
PP RUEHLA
DE RUEHMD #0485/01 1391456
ZNY CCCCC ZZH
P 191456Z MAY 09
FM AMEMBASSY MADRID
TO RUEHC/SECSTATE WASHDC PRIORITY 0651
INFO RUEHLA/AMCONSUL BARCELONA 3984
RUEAIIA/CIA WASHDC
RUEHNA/DEA HQS WASHDC
RUEAWJA/DEPT OF JUSTICE WASHDC
RUEATRS/DEPT OF TREASURY WASHDC
RHEFDIA/DIA WASHDC
RUCNFB/FBI WASHDC
RUEAHLC/HOMELAND SECURITY CENTER WASHINGTON DC
RUEILB/NCTC WASHINGTON DC
RHEFHTA/TSA HQ WASHINGTON DC
RUCNSE/US SECRET SERVICE WASHDC

C O N F I D E N T I A L SECTION 01 OF 05 MADRID 000485

SIPDIS

FOR EUR/WE'S ELAINE SAMSON AND STACIE ZERDECKI
FOR S/CT'S HILLARY BATJER JOHNSON AND PAUL SCHULTZ,
PASS TO NCTC
PASS TO DHS

E.O. 12958: DECL: 05/11/2019
TAGS: KVPR PTER PREL PGOV CVIS ASEC KHLS SP
SUBJECT: UPDATE ON SPAIN'S INFORMATION COLLECTION,
SCREENING AND SHARING PRACTICES

REF: A. SECSTATE 32287
¶B. 07 MADRID 2055
¶C. MADRID 484

Classified By: Charge d'Affaires William H. Duncan for reasons 1.4 (b),
(c) and (d)

¶1. (SBU) In response to REFTEL A, Embassy Madrid offers the following update to responses on Spain's information collection, screening and sharing practices for terrorist screening purposes. For ease of reading, Post has rewritten the questions in each of the eight categories. REFTEL B, which provides Post's original responses to the pilot running of this project in 2007, provided comprehensive answers to most of the questions below. In assembling its updated responses, Post -- among other things -- drew from the answers that the Embassy's inter-agency team and, separately, the GOS recently prepared in response to questionnaires created by the DHS regarding the Visa Waiver Program.

//Immigration Data Bases and Traveler Information Collection//

¶2. (SBU) Q: What computerized immigration databases are used to track entries and exits?
-- Is the computerized immigration database available at all ports of entry (POEs)? If immigration databases are available at some POEs, but not all, how does the host government decide which POEs will receive the tool?
-- What problems, if any, limit the effectiveness of the systems? For example, limited training, power brownouts, budgetary restraints, corruption, etc.?
-- How often are national immigration databases updated?
-- What are the country's policies (legislation, mandates, etc.) on collecting information from travelers arriving in the country?
-- Are there different policies for entry and exit at air, sea, and land POEs and for domestic flights?
-- What agency oversees the collection of traveler information?
-- What are the policies of the collecting agency to share that information with foreign governments?
-- Does the host government collect Passenger Name Record (PNR) data on incoming commercial flights or vessels? Is this data used for intelligence or law enforcement purposes to screen travelers in a systematic

way? Does host government have any existing treaties to share PNR data?
-- If applicable, have advance passenger information systems (APIS), interactive advanced passenger information systems (IAPIS), or electronic travel authority systems been effective at detecting other national security threats, such as wanted criminals?

¶3. (C) A: Post notes that the GOS experiences problems with compliance, because receiving the transmission of traveler information data from the airlines on short notice makes it difficult to do the time-consuming checks to vet the names in time. The Spanish system also generates a considerable amount of false positives. Spain is a pioneer among European countries in the use of the APIS system, but a lot of work still needs to be done. The GOS does not collect PNR data on incoming commercial flights or vessels. The official GOS policy is that all passports are supposed to be scanned upon arrival, but in practice this does not always happen. Spain does now have the APIS system.

//Watchlisting//

¶4. (SBU) Q: Is there a name-based watchlist system used to screen travelers at POEs?
-- What domestic sources of information populate the name-based watchlist, i.e. names of deported persons, terrorist lookouts, criminal wants/warrants? If host government maintains a watchlist, how many records does the watchlist contain, and how many are terrorist-related?

-- Which ministry or office maintains the watchlist?
-- What international watchlists do the host government use for screening individuals, e.g. Interpol or TSA No Fly lists, UN, etc.?
-- What bilateral/multilateral watchlist agreements exist between host government and its neighbors?

¶5. (C) A: The GOS has implemented the Schengen Information System (SIS) mentioned in Para 2 of REFTEL B.

//Biometrics//

¶6. (SBU) Q: Are biometric systems in place at ports of entry (air, land, sea)? If no, does host government have plans to install such a system? If biometric systems are available at some POEs, but not all, how does the host government decide what POEs will receive the tool?
-- What biometric technologies, if any, does the host government use, i.e. fingerprint identification, facial recognition, iris recognition, hand geometry, retinal identification, DNA-based identification, keystroke dynamics, gait analysis? Are the systems ICAO compliant?
-- Are biometric systems integrated for all active POEs? What are the systems and models used? Are all passengers screened for the biometric or does the host government target a specific population for collection (i.e. host country nationals)? Do the biometric collection systems look for a one to one comparison (ensure the biometric presented matches the one stored on the e-Passport) or one to many comparisons (checking the biometric presented against a database of known biometrics)?
-- If biometric systems are in place, does the host government know of any countermeasures that have been used or attempted to defeat biometric checkpoints?
-- What are the host government's policies on collecting the fingerprints of travelers coming into the country?
-- Which agency is responsible for the host government's fingerprint system?
-- Are the fingerprint programs in place NIST, INT-I, EFTS, UK1 or RTID compliant?
-- Are the fingerprints collected as flats or rolled?
-- Which agency collects the fingerprints?

¶7. (C) A: The GOS recently reported to the USG that, as of early 2009, not all passport readers currently deployed at Spain's international airports and seaports are capable of reading the biometric information contained in the chip of ICAO-compliant e-passports. The GOS reported that this rollout currently is underway, in accordance with EU norms. Meanwhile, the GOS has started to take fingerprints with the implementation of the SIS border controls and is supposed to be taking 10-digit fingerprints. The SAID II upgrade of Spain's national fingerprint system, mentioned in REFTEL B, is now operational, according to Post's LEGAT Office.

//Border Control and Screening//

¶8. (SBU) Q: Does the host government employ software to screen travelers of security interest?
-- Are all travelers tracked electronically, or only non-host- country nationals? What is the frequency of travelers being "waived through" because they hold up what appears to be an appropriate document, but whose information is not actually recorded electronically? What is the estimated percentage of non-recorded crossings, entries and exits?
-- Do host government border control officials have the authority to use other criminal data when making decisions on who can enter the country? If so, please describe this authority (legislation, mandates, etc).
-- What are the host government's policies on questioning, detaining and denying entry to individuals presenting themselves at a point of entry into the country? Which agency would question, detain, or deny entry?
-- How well does information sharing function within the host

government, i.e., if there is a determination that someone with a valid host-government visa is later identified with terrorism, how is this communicated and resolved internally?

¶9. (C) A: The GOS "Verifier" database mentioned in Para 4 of REFTEL B is now implemented. Meanwhile, the GOS in early 2009 reported to the USG that all of Spain's border crossing points (e.g., international airports and seaports with external Schengen borders) are equipped with Optical Character Recognition (OCR) passport readers, which are connected to police databases. The GOS also highlighted to the USG that, as part of the EU "Aeneas Program" Spain in 2008 established Operation "Seahorse Network," which is a a satellite-based network which enable secure communications between Spain, Portugal, Morocco, Mauritania, Senegal, and Cape Verde to combat illegal immigration. The GOS informs the USG that it anticipates establishing in Madrid a National Center for Maritime Border Control, which will have four regional centers: Atlantic, Strait of Gibraltar, Mediterranean, and Bay of Biscay.

//Passports//

¶10. (SBU) Q: Does the host government issue a machine-readable passport containing biometric information? If so, what biometric information is included on the document, i.e. fingerprint, iris, facial recognition, etc.? If not, does host government plan to issue a biometric document in the future? When?
-- If the host government issues a machine-readable passport containing biometric information, does the host government share the public key required to read the biometric information with any other governments? If so, which governments? Does the host government issue replacement passports for full or limited validity (i.e. the time remaining on the original passports, fixed validity for a replacement, etc.)?
-- Does the host government have special regulations/procedures for dealing with "habitual" losers of

passports or
bearers who have reported their passports stolen multiple
times?
-- Are replacement passports of the same or different
appearance and page length as regular passports (do they
have something along the lines of our emergency partial
duration passports)?
-- Do emergency replacement passports contain the same or
fewer biometric fields as regular-issue passports?
-- Where applicable, has Post noticed any increase in the
number of replacement or "clean" (i.e. no evidence
of prior travel) passports used to apply for U.S. visas?
-- Are replacement passports assigned a characteristic number
series or otherwise identified?

¶11. (C) A: Spanish Embassy and Consulates no longer provide replacement or limited validity passports, both of which are now exclusively provided by the Ministry of Foreign Affairs' Directorate General for Consular Services. In early 2009, the GOS reported to the USG that, since January 1, 2006, 786 blank Spanish passports had been lost or stolen while 160,462 personalized passports issued by the GOS had been reported lost or missing. The GOS reported that it provides, via Internet, data on all lost, stolen, or misappropriated passports to Interpol's Stolen and Last Travel Document (SLTD) Database. The specific information it provides includes personal data, the number, expiration and validity dates of the passport.

//Fraud Detection//

¶12. (SBU) Q: How robust is fraud detection and how actively are instances of fraud involving documents followed up?
-- How are potentially fraudulently issued documents taken out of circulation, or made harder to use?

¶13. (C) A: In early 2009 the GOS reported to the USG on Spain's procedures for taking fraudulent documents out of circulation The person traveling with the fraudulent travel document is rejected at the Spanish border and returned to their country of departure. According to the GOS, in all cases the documents are photocopied and the original rejected documents are sent, along with a standard EU form, to the authorities in the country to which the traveler has been returned. They GOS reports that it is necessary to send the fraudulent travel document to the authorities in the country to which the travel has been returned, otherwise the rejection is not accepted by the other government. The GOS claims the fraudulent document is never returned to the traveler.

//Privacy and Data Security//

¶14. (SBU) Q: What are the country's policies on records related to the questioning, detention or removal of individuals
encountered at points of entry into the country? How are those records stored, and for how long?
-- What are the country's restrictions on the collection or use of sensitive data?
-- What are the requirements to provide notice to the public on the implementation of new databases of records?
-- Are there any laws relating to security features for government computer systems that hold personally identifying information?
-- What are the rules on an individual's ability to access data that homeland security agencies hold about them?
-- Are there different rules for raw data (name, date of birth, etc.) versus case files (for example, records about enforcement actions)?
-- Does a non-citizen/resident have the right to sue the government to obtain these types of data?

¶15. (SBU) A: Post does not have any updates for this

category.

//Identifying Appropriate Partners//

¶16. (SBU) Q: Department would appreciate post's in-house assessment of whether host government would be an appropriate partner in data sharing. Considerations include whether host government watchlists may include political dissidents (as opposed or in addition to terrorists), and whether host governments would share or use U.S. watchlist data inappropriately, etc.
-- Are there political realities which would preclude a country from entering into a formal data-sharing agreement with
the U.S.?
-- Is the host country's legal system sufficiently developed to adequately provide safeguards for the protection and nondisclosure of information?
-- How much information sharing does the host country do internally? Is there a single consolidated database, for example? If not, do different ministries share information amongst themselves?
-- How does the country define terrorism? Are there legal statutes that do so?

¶17. (C) A: The USG, led by DHS, currently is engaging the GOS on signing a bilateral agreement on Preventing and Combating Serious Crime (PCSC, See REF C). This initiative has been blessed by the inter-agency process and has Circular 175 authority. The draft PCSC agreement provides for the sharing -- including query ability -- of extensive information, including DNA profiles and fingerprinting data as well as personal data. DHS and Post in recent months have shared the draft agreement with the GOS, which thus far has responded favorably. Post understands that the USG would like this agreement to be signed before the end of 2009. Spain's Minister of Interior, Alfredo Perez Rubalcaba, will

likely discuss this issue in his meetings with DHS Secretary Napolitano during his upcoming visit to Washington, tentatively scheduled for June 24-26. (See forthcoming SEPTEL.)
DUNCAN